We Claim:

1. A method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of said participants includes a memory and having a respective private key t, a and public key Y_t, Y_c stored therein, said public keys derived from a generator α and a respective ones of said private keys t, a, said method comprising the steps of:

(a) a first of said participants generating a unique transaction identification information PID upon initiation of said electronic transaction;

(b) said first participant forwarding to a second participant said transaction identification information PID and a first certificate C1, said first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information TIU ID unique to said first participant and said public information Y_t of said first participant;

(c) said second participant verifying said first certificate C1, according to said predetermined algorithm, upon receipt thereof and extracting said identification information TIU ID and said public information Y_t therefrom;

(d) said second participant, upon verification of said first certificate C1, generating first and second random integers R2 and R3, respectively;

(e) said second participant generating a third random integer k and computing a session parameter α^k by exponentiating a function including said generator to a power k and exponentiating said public key Y_t to a power k to produce a session key Y_t^k;

(f) said second participant generating a first signature component r1 by signing said transaction identification information PID utilizing said public key Y_t of said first participant and generating a second signature component s1 by signing said first random integer R2 utilizing said private key a of said second participant, said signatures being generated according to a predetermined protocol;

(g) said second participant forwarding a message to said first participant, including said signature components r1, s1 and a second certificate C2 signed by said certification

authority according to a predetermined algorithm and including an identification information CID unique to said second participant and said public information Yc of said second participant;

(h) said first participant verifying said second certificate C2 and extracting said identification information CID and public key Y_c and verifying the authenticity of said second participant by extracting said transaction identification information PID from said received message and comparing said received transaction identification information PID to said transmitted value;

(i) said first participant extracting said first random integer R2 from said received message and transmitting said first random integer R2 to said second participant to acknowledge verification of said second participant;

(j) said second participant verifying the authenticity of said first participant by comparing said received first random integer R2 to said generated first random integer R2 and transmitting said second random integer R3 to said first participant to acknowledging verification of said first participant, thereby permitting exchange of information between said participants.

3. A method as defined in claim 1, wherein said first participant forwards a transaction amount TA with said identification PID.

4. A method as defined in claim 1, wherein said first signature component r1 combines said session key Y_t^k and a message M2, indicative of the concatenation of said identification information TIU ID, said first random information R2, and said transaction identification information PID.

5. A method as defined in claim 3, wherein said first signature component r1 is of the form $M2 * Y_t^k \bmod L$.

6. A method as defined in claim 3, wherein said second signature component s1 is of the form h*a + k mod q, where q is the order of an elliptic curve, h is a hash of the concatenation of said second random integer R3, said session parameter α^k and said message M2.

7. A method as defined in claim 5, including in step (g) of claim 1 forwarding said hash to said first participant.

8. A method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of said participants includes a memory and having a respective private key t, a and public key Y_t, Y_c stored therein, said public keys derived from a generator α and a respective ones of said private keys t, a, said method comprising the steps of:

(a) a first of said participants generating a unique transaction identification information PID upon initiation of said electronic transaction;

(b) said first participant forwarding to a second participant said transaction identification information PID and a first certificate C1, said first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information TIU ID unique to said first participant and said public information Y_t of said first participant;

(c) said second participant verifying said first certificate C1, according to said predetermined algorithm, upon receipt thereof and extracting said identification information TIU ID and said public information Y_t therefrom;

(d) said second participant, upon verification of said first certificate C1, generating a first random integer R2;

(e) said second participant generating a first and second signature components r1, s1 utilizing said public key Y_t of said first participant and said private key a of said second participant, respectively according to a predetermined protocol;

(f) said second participant forwarding a message to said first participant, including said signature components r1, s1 and a second certificate C2 signed by said certification authority according to a predetermined algorithm and including an identification information CID unique to said second participant and said public information Yc of said second participant;

(g) said first participant verifying said second certificate C2 and extracting said identification information CID and public key Y_c and verifying the authenticity of said second participant by extracting said transaction identification information PID from said received message and comparing said received transaction identification information PID to said transmitted value;

(h) said first participant extracting said first random integer R2 from said received message and transmitting said first random integer R2 to said second participant to acknowledge verification of said second participant; and

(i) said second participant verifying the authenticity of said first participant by comparing said received first random integer R2 to said generated first random integer R2 and transmitting a second random integer R3 to said first participant to acknowledging verification of said first participant, thereby permitting exchange of information between said participants.